Network Security Vulnerabilities Heading for Malicious Attack

Mohd. Izhar
HMR Inst. of Tech. & Mgt,
GGSIP UNIVERSITY, DELHI
Ph.D. SCHOLAR OF MEWAR
UNIVERSITY, NH-79,
Gangrar, Chittorgarh
(Rajasthan) India

Mohd. Shahid
PDM College of Engg.,
Bahadurgarh, MD University,
Ph.D. SCHOLAR OF MEWAR
UNIVERSITY, NH-79,
Gangrar, Chittorgarh
(Rajasthan) India

V.R.Singh
PDM College of Engg.
Bahadurgarh, MD University,
MEWAR UNIVERSITY
NH-79, Gangrar, Chittorgarh
(Rajasthan) India-312901

ABSTRACT
An organization requires that WLAN must address three critical areas: Data Confidentiality and Integrity, Authentication and Access Control and Intrusion Detection and Prevention. By the growth of Wireless Network, so many security threats have also been raised that does not require much expertise and expensive equipment to launch an attack against an organization. Such attacks are initiated from inside or outside at a great distance using readily available standard wireless equipment. These days the WLAN system is migrating from Pre-RSNA methods of Security to the RSNA and using WPA/WPA2 with AES encryption, in conjunction with 802.1x authentication for providing a security to WLANs and at the same time wireless intrusion detection and prevention systems are being made more capable and easier to manage but still wireless security solution in place are vulnerable to malicious attacks and need to be kept reviewed as per standard of IEEE as well of Wi-Fi Alliance and beyond it. WLAN vendors and researchers look into it and try to ensure the solution to the problem.

MAC address spoofing refers to the getting the MAC address of other network card and using it on the network for misrepresentation and illegitimate use. This paper helps the community at large in knowing several security tools. These tools scan whole network and provide various information of node(s) within the node to the malicious node (attacker), the node which intend to attack the network and spoof MAC address and breaches the security. This MAC address is continuously sent over at Wi-Fi networks, even if they use secure WEP/WPA Encryption. The node with fake MAC address masquerade as an authorized wireless access point or as an authorized client. Such node launches denial of service attacks, bypass access control mechanisms, or falsely advertise services to wireless clients.

Keywords
RSNA (Robust Security Network Association) WPA (Wireless Protected Access) Carrier Sense Multiple Access/Collision Avoidance(CSMA/CA), Counter mode with Cipher-block chaining Message authentication code Protocol (CCMP), temporal key integrity protocol(TKIP), confidentiality, Wireless Local Area Network(WLAN) local area network, Medium Access Controller(MAC) and Physical (PHY).

1. INTRODUCTION
Public wireless networks are convenient, but it is dangerous if they do not employ current RSNA methods of network security that are standardized by IEEE and Wi-Fi alliance even if they are properly secured by making use of these standards, connecting to them might be risky. Whenever possible, one must connect to wireless networks that require a network security key or have some other form of security, such as a certificate [1]. The information sent over such networks is encrypted.

It protects the connecting devices from unauthorized access. If one connects to a network that's not secure, it is possible that any malicious node with the right tools can easily know everything and it can do that one do on his/her device, sees websites and the files he/she send and receive, the user names and passwords one use for log-in purpose even personal information such as bank records, online banking passwords, statements of accounts and important data are not secure in such unsecured network. Security is also required for a wireless network one owns, it is important because the network's signal go beyond the boundaries of home and organization [2]. The nodes, nearby of such network might be able to access the information stored on authorized nodes and can use Internet connection to log on the web.

A device that connects to a network requires internal or external wireless network adapter or network interface card(NIC). In MAC spoofing the physical address hardwired in NIC is the main point of vulnerability. Efforts are made to point out such weakness and provide its countermeasure [2]. A network attacker can use a protocol analyzer to know a valid MAC address[15].

2. BACKGROUND
Primary factors for security in a wireless environment are: 1. Theft: Unauthorized users often try stealing data. 2. Access Control: Wireless networks have all the same access control vulnerabilities as wired networks; even it can be easily targeted. 3. Authentication: Unauthorized users can also log onto them illegally. 4. Encryption : Wireless routers support medium and strong levels of encryption 5. Protection: The best protection is to become familiar with WLAN and wireless router.

Proper measures are : Older wireless network points have two basic security methods: MAC address filtering and Wired Equivalent Privacy (WEP)[5]. Both MAC and WEP offer only very basic security and the risks are associated with them. Newer versions of wireless network points make use of 2 additional security methods. The first is the Wireless Application Protocol (WAP), of which there are several variations. An access point may also support the Remote Authentication Dial In User Service (RADIUS), a protocol that works in conjunction with Network Operating Systems

such as Windows, UNIX or Linux servers. Wireless LANs, because of their broadcast nature, require the addition of: • User authentication to prevent unauthorized access to network resources • Data privacy to protect the integrity and privacy of transmitted data.

The 802.11 specification stipulates two mechanisms: 1. open authentication and 2.shared key authentication. Two other mechanisms: the Service Set Identifier (SSID) and authentication by client Media Access Control (MAC) address are also commonly used. MAC address spoofing is possible in 802.11 network interface cards (NICs) that allow the universally administered address (UAA) to be overwritten with a locally administered address (LAA)[6]. A network attacker can use a protocol analyzer to determine a valid MAC address. Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. Since the approval of the IEEE 802.11-2007, Revision of IEEE Std 802.11-1999, Security on their wireless networks has been improved by making use of CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code protocol). CCMP uses AES (Advanced Encryption Standard) as opposed to the RC4 streaming cipher found in implementations of WEP (Wired Equivalent Privacy) and TKIP (Temporal Key Integrity Protocol).

MAC spoofing is an important technique which can be beneficial for some reasons as some Internet Service Provider bind their services to a specific MAC address if NIC damages the users can change with New NIC and spoof it as old one [2, 7]. Similarly some software licenses are bound to a specific Mac address and thus require MAC spoofing in case of damage of old one.

But at the same time some vulnerability is taken into account as its negative effects. These are as follows [2, 7]:

1. MAC spoofing can be done to get access of wireless network.
2. MAC spoofing can be result in illegitimate use of Wireless Network for any kind of crime.
3. Internet Service Provider bind their services to a specific MAC address, unauthorized node may access of the service by using MAC address of authorised user.
4. Some software licences are based on MAC address, one malicious node uses it as authentic user.

These are very well known vulnerabilities but the problem is that one is not able to solve the problem because:

1. It is possible to track illegal Internet traffic to a specific IP and to retrieve the name and address of the IP's registrant, not of the illegal MAC spoofer.
2. MAC address is continuously being sent over Wi-Fi networks, even if they use secure WEP/WPA Encryption.
3. Impact of MAC spoofing is that approximately 50% of all traffic that is required to go to the default gateway but goes to targeted computer. The remaining client on the network will be unable to communicate with their default gateway.
4. Mac address filtering is also no solution for the organization.

But even some solutions are there to solve the problem of MAC spoofing:

1. OS can check the MAC address entries and delete it automatically if there is some change in it.
2. MAC address at ARP can be compared with that of MAC address through OS whenever packets arrive to it
3. MAC address are stored in OS and received from OS, it can be checked directly from NIC.
4. Association of MAC address with IP address can solve the problem.
5. Encryption of the communication between the wireless PC and access point can also be used as a solution to the problem.

3. TOOLS AND MTHODS

An Intruder has several ways to attack on a wireless network. The easiest method of attack is MAC spoofing by which malicious node can impersonate as an authorized wireless access point or as an authorized client. It can launch denial of service attacks, bypass access control mechanisms, or falsely advertise services to wireless clients. There are several tools by which one can come to know the physical address of any node in the network. These IP Scanner is a free, fast and easy-to-use network scanner. IP Scanner is able to locate all the computers on wired or wireless local network and conduct a scan of their ports. It can detect all the IP addresses on any Wi-Fi network. Even advanced IP Scanner, can wake up and shut down remote groups of Windows machines. The list are as follows : Advanced IP Scanner 2.2.224, Colasoft MAC Scanner Pro 2.2, Angry IP Scanner 2.x, IPScan-II.The tool which has been used for scanning the network is free open source Angry IP scanner[15].

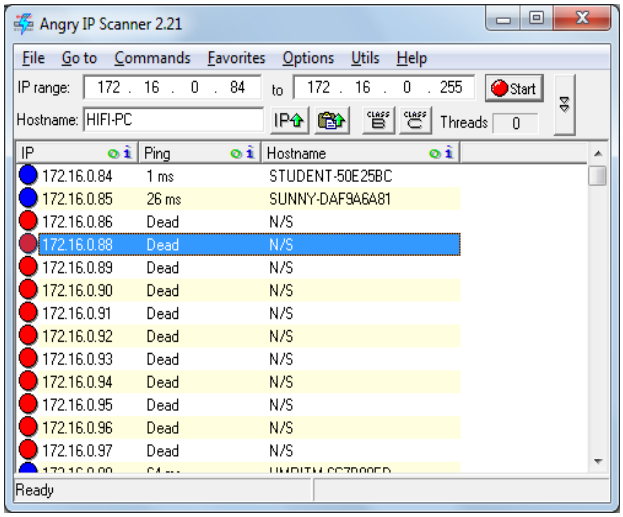

Fig. 1: Scanning Result of Angry IP Scanner

It is a very fast IP address and port scanner. It can scan IP addresses in any range as well as any their ports. It is cross-platform and lightweight. Angry IP scanner simply pings each IP address to check if it's alive, then optionally it is resolving its hostname, determines the MAC address, scans ports, etc. It also has additional features, like NetBIOS information (computer name, workgroup name, and currently logged in Windows user), favorite IP address ranges, web server detection, customizable openers, etc. There are currently two different versions available: New cross-platform version, 3.x - still in beta, Old Windows-only version, 2.x. which can be used for scanning purpose.

SMAC is a powerful MAC Address Spoofer for Windows 7, VISTA, 2008, 2003, XP, 2000 systems. SMAC is developed by Certified Professionals (CISSP, CISA, CIPP, and MCSE SMAC capabilities are: 1. Automatically Activate new MAC Address right after changing it. 2. Show the manufacturer of the MAC Address. 3. Randomly generate any New MAC Address or based on a selected manufacturer. 4. Pre-load MAC Addresses List and choose the new MAC address from the list[11].

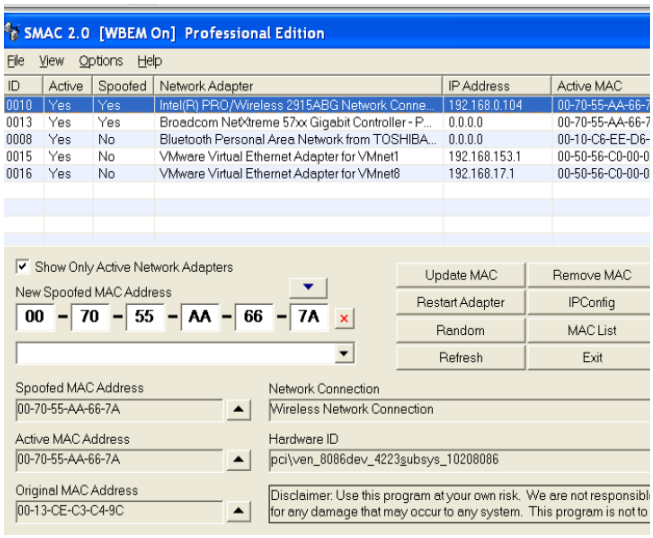

Fig. 2 : SMAC Address Changer

Technitium MAC Address Changer or TMAC can change (spoof) Media Access Control (MAC) Address of Network Interface Card (NIC) or Wireless Network Card (Wi-Fi), irrespective of the NIC's drivers or its manufacturer[10]. It has many new features which can to change IP Address, Gateway, DNS Servers, IPv6 support, enable/disable DHCP in one click, network configuration presets and also many other features.

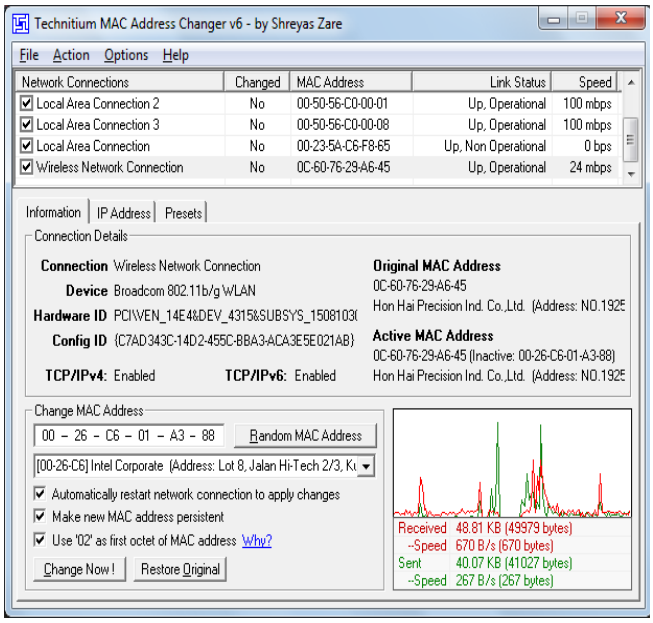

Fig. 3: TMAC Address Changer

OPNET Technologies is a software business organization that provides performance analysis for computer networks and applications. OPNET is leader in the modeling, simulation, and analysis of strategic and tactical defence communications networks and net-centric applications. OPNET provides simulator for an in-depth understanding of networking technologies and protocols (e.g., IP, IPv6, HAIPE, LTE, MANET, MPLS, QoS, VoIP, and VPN, etc.), optimization techniques, and best practice methodologies in constructive modelling. OPNET IT Guru Academic Edition is a utility designed with educational purposes in mind, specifically to help users be introduced to the domain of networking. By the use of OPNET IT Guru Academic Edition a simulation test bed scenario has bee created for WLAN[16].

4. RESULTS AND DISCUSSION

4.1 Testbed

A typical scenario of WLAN is developed in which different nodes are considered connecting through an access points. A WLAN includes a leased line or wired internet at the back, the same is connected to the server through router and various access points are connected through different switches. These access points are points where WLAN users log-on to connect the nets. The present testbed can try to spoof the access points as well any nodes.

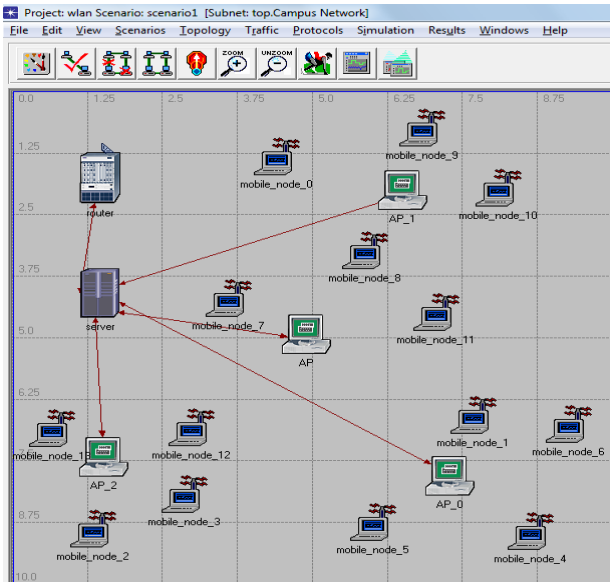

Fig. 4: Typical WLAN Scenario

A free open source Angry IP scanner scans the WLAN network and shows dead and alive nodes with their MAC Address that means providing various information of node(s) to the malicious node (attacker) that may result in MAC address spoofing and in turn breaching the security.

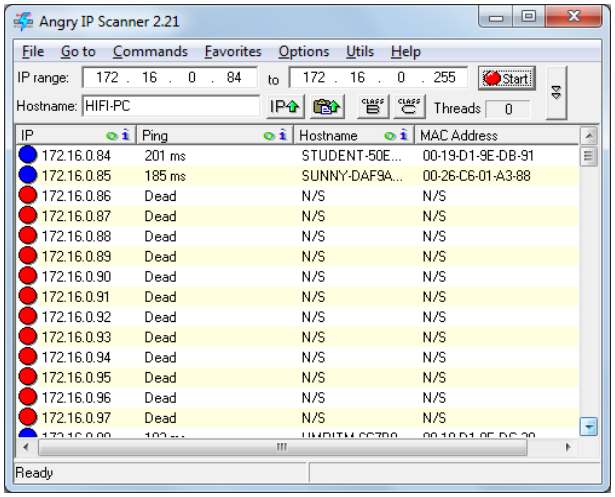

Fig. 5: IP Scanner shows MAC Address

Advanced ip scanner has also been used and they provide more advanced features which on the one hand are very useful for the Tester for WLAN networks but handy information also hackers. The problem is that MAC address is continuously being sent over Wi-Fi networks, even WEP/WPA Encryption technique is being used that means no security from such spoofing.

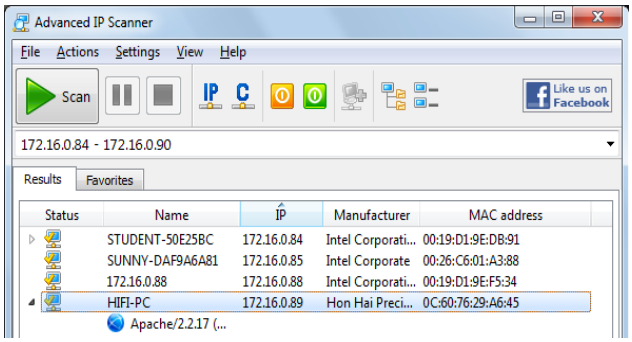

Fig. 6: Advanced IP Scanner

4.2 Scanning Test

Ping and arp tables produce the same test result and shows that such scanner are trust worthy for positive scanning for ethical hackers as well for intruders

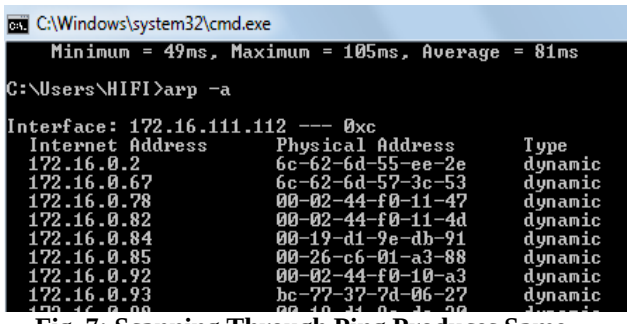

Fig. 7: Scanning Through Ping Produces Same Result.

4.3 Spoofing

There are various ways by which one can easily change the MAC address as desired. Typically following 3 ways are common:

1. One can change the MAC address through device manager of the System.

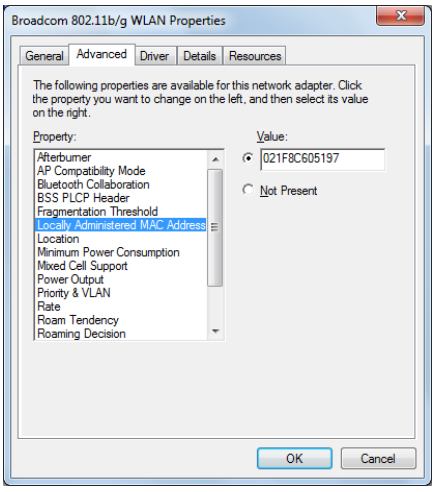

Fig. 8: Changing MAC Address through Device Manager

2. One can also change the MAC address through editing the Registry of the System. The Method is shown through the following picture:

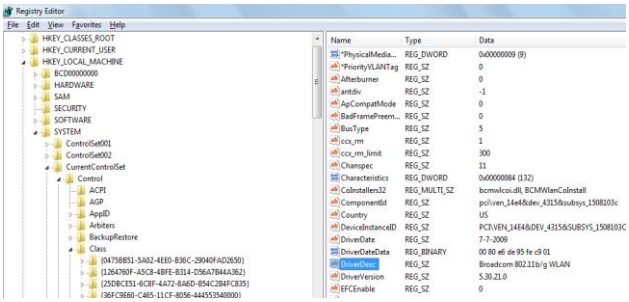

Fig. 9: MAC Changing through Registry Editor

3. The MAC address can be changed through the MAC address Changer such as TMAC and SMAC softwares. The Changed MAC address has been show through the following picture.

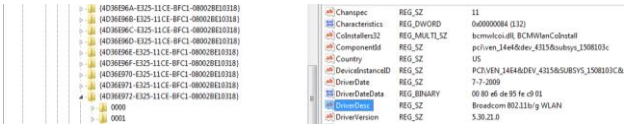

Fig. 10: MAC Address change in just one Minute

The changed MAC address can be verified through IPCONFIG /ALL command at the DOS prompt.

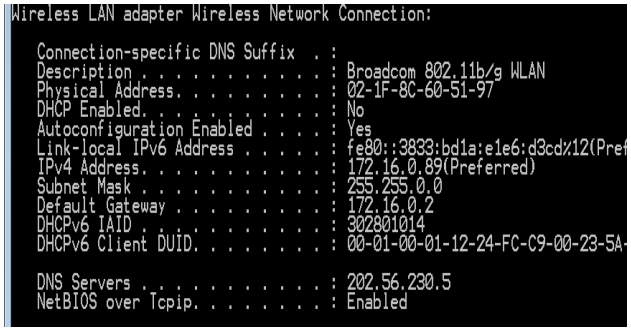

Fig. 11: Verification of Changed MAC address

The same can also be verified through IP scanner used earlier.

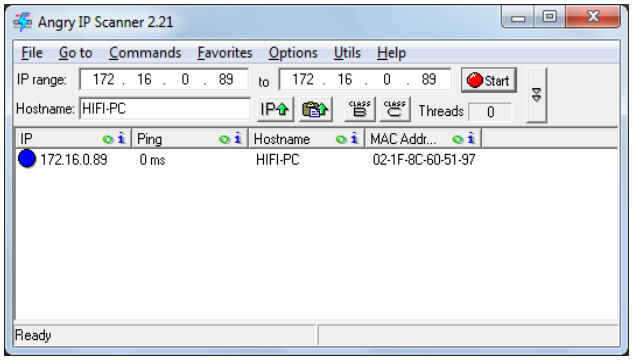

Fig. 12: Spoofed MAC Address at WLAN

The Changed MAC address of malicious node is not traceable the other node or server in the same wireless network catches the fake address of the malicious unauthorized node as the authorized legitimate user. The following result captured through author node points out the same.

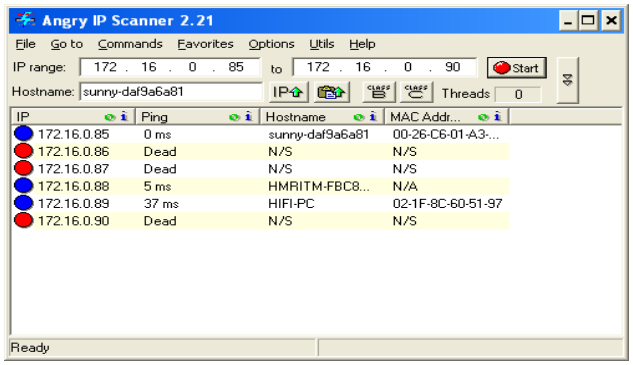

Fig. 13: Malicious Node having Spoofed Address

5. CONCLUSION

There is always question "Are we really safe while on WLAN" ? The answers to this question varies according to WLAN scenario. Typically WLAN may be in one of the form : Home and SOHO WLAN security, Small Business WLAN security, Medium to large Enterprise WLAN security, Military grade maximum level WLAN security. The Security actually depends on what kind of security WLAN groups requires. Sometimes data is of utmost important and need high security and cost to it does not matter. The standardized method for small business WLAN is 802.1x and PEAP or TTLS authentication. EAP-TLS or PEAP-EAP-TLS using "soft" Digital Certificates (certificates that are stored on the user's hard drive) would be the recommended authentication method for Medium to large Enterprise security level.

In Military grade maximum level WLAN security, the certificates is stored inside an HSM (Hardware Security Modules also known as Cryptographic Modules for server side applications, that costs thousands of dollars in the form of a tamper resistant external module) which are typically in the form of a USB dongle of the size of two fingers carried on a person's key chain or a smartcard.

To conclude, This paper suggest the way for Home and Small Office WLAN that secure such network from various threats as pointed out. Surely. These solutions are economical and methods are: OS need to be dynamic. MAC address at ARP can be compared with that of MAC address through OS. MAC addresses are to be checked directly from NIC. Association of MAC address with IP address can solve the problem and also encryption of the communication between the wireless PC and access point can also be used as a solution to the problem.

6. ACKNOWLEDGMENTS

Our sincerely thanks to the management of HMR Institute of Technology, PDM College of Engineering and Mewar University who supported the most in preparing this document.

7. REFERENCES

[1] Turkan Ahamad & Manar Younis, IJCA (0975 – 888), Volume 48– No.16, June 2012. The Enhancement of Routing Security in Mobile Ad-hoc Networks.

[2] Payal Pahwa, Gaurav Tiwari, Rashmi Chhabra, *IJAEA, Jan. 2010*. Spoofing Media Access Control (MAC) and its Counter Measures.

[3] Farhad Soleimanian & Zeinab Abbasi, IJCA(0975 – 888), Volume 47– No.22, June 2012. Analysis and Evaluation of Dynamic Load Balancing in IEEE 802.11b Wireless Local Area.

[4] Joshua Wright, 2003. Detecting Wireless LAN MAC Address Spoofing.

[5] Fanglu Guo and Tzi-cker Chiueh, 2005. Sequence Number-Based MAC Address Spoof Detection.

[6] Stuart Compton, SANS Institute, May 2007. 802.11 Denial of Service Attacks and Mitigation.

[7] D. Gupta, G. Tiwari,Y. K and P. Kumar, IJRTE 2009.Media Access Control (MAC) MAC spoofing and its countermeasures.

[8] Siemens Enterprise Communications, July 2008. WLAN Security Today: Wireless more Secure than Wired, white paper.

[9] George Ou, Jan 3, 2005. Wireless LAN security guide.

[10] Website, http://www.technitium.com/

[11] Website, http://www.klcconsulting.net/smac.

[12] Website, http://www.softpedia.com/ get/ Network-Tools/ IP-Tools/ IPScan-II.shtml

[13] Website, http://ip-scan.qarchive.org/, May 2012

[14] Website, ww.radmin.com/products/ipscanner/, May 2012

[15] Website, http://www.angryip.org/w/Home, May 2012

[16] Website, http://www.opnet.com/itguru-academic

[17] Richa Bansal, Siddharth Tiwari, Divya Bansal, ICON 2008: 1-6. Non-cryptographic methods of MAC spoof detection in wireless LAN.

[18] Guenther Lackner, Udo Payer, and Peter Teu, January 20, 2009. Combating Wireless LAN MAC-Layer Address Spoofing with Fingerprinting Methods.

[19] Hassene Bouhouche & Sihem Guemara, IJCA (0975 – 8887), Volume 6– No.3, September 2010. A QoS-based Resources Reservation Mechanism for Ad Hoc Networks.

[20] IEEE Std 802.11™-2007, Revision of IEEE Std 802.11-1999, IEEE 3 Park Avenue New York, NY 10016-5997, USA 12 June 2007.

[21] IEEE Std. 2009 Revision of IEEE Std 802.11™-2007, 30 sept. 2009.

[22] IEEE Std 802.11i-2004, Amendment to IEEE Std 802.11™, 1999 Edition (Reaff 2003) as amended by IEEE Stds 802.11a™-1999, 802.11b™-1999,802.11b™-1999/Cor 1-2001, 802.11d™-2001, 802.11g-2003, and 802.11h-2003] Amendment 6: Medium Access Control (MAC) Security Enhancements, 23 July 2004.